29/03
406

PCT/EP00/09256
10/088622

Europäisches Patentamt | European Patent Office | Office européen des brevets

REC'D 05 FEB 2001
WIPO PCT

EP00/9256

4

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

99402299.4

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

BEST AVAILABLE COPY

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

Hatten

I.L.C. HATTEN-HECKMAN

DEN HAAG, DEN
THE HAGUE, 25/01/01
LA HAYE, LE

EPA/EPO/OEB Form 1014 - 02.91

THIS PAGE BLANK (USPTO)

Europäisches Patentamt
European Patent Office
Office européen des brevets

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.:
Application no.: 99402299.4
Demande n°:

Anmeldetag:
Date of filing: 20/09/99
Date de dépôt:

Anmelder:
Applicant(s):
Demandeur(s):
THOMSON multimedia
92100 Boulogne Billancourt
FRANCE

Bezeichnung der Erfindung:
Title of the invention:
Titre de l'invention:
Method for device registration in a wireless home network

In Anspruch genommene Prioriät(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat: State: Pays:	Tag: Date: Date:	Aktenzeichen: File no. Numéro de dépôt:

Internationale Patentklassifikation:
International Patent classification:
Classification internationale des brevets:
/

Am Anmeldetag benannte Vertragstaaten:
Contracting states designated at date of filing: AT/BE/CH/CY/DE/DK/ES/FI/FR/GB/GR/IE/IT/LI/LU/MC/NL/PT/SE/TR
Etats contractants désignés lors du depôt:

Bemerkungen:
Remarks:
Remarques:

Method for device registration in a wireless home network

The invention concerns a method for the registration of a device in a wireless home network. The invention can be used in the frame of a network based on the IEEE 1394 – 1995 serial bus standard, but is not necessarily limited to such an environment.

The IEEE 1394 bus is a wired bus, and suffers from inherent drawbacks: it uses a cable, which is a restriction by itself compared to a wireless product, and the cable length between two devices is limited to 4.5 meters. The introduction of wireless transmissions in a IEEE 1394 – 1995 based network is of an obvious interest. This topic is covered by the European ETSI BRAN project that is standardizing a wireless 1394 network in the 5 GHz band, under the title 'Hiperlan type 2'.
Hiperlan 2 is a layered standard defining a PHY layer (OSI level 1), a DLC layer (OSI level 2), and a few Convergence Layers for some core network technologies (ATM, Ethernet, IEEE 1394...).

Hiperlan 2 proposes a security scheme based on authentication and encryption. This security scheme allows to restrict the access of the network to only allowed users. Hiperlan 2 is initially targetting business applications (corporate LANs), and thus can rely on a certain network management infrastructure. Hiperlan 2 requires for its authentication procedure that both the Mobile Terminal ('MT') and the AP/CC (Access Point – Central Controller) have a shared secret (an 'authentication key') prior to the authentication procedure. This authentication key is communicated to both the MT and the AP during network installation by the network manager.

In a home environment, it is not appropriate to rely on the user to perform such installation operations. The purpose of the present invention is to

propose a method using mechanisms already specified in Hiperlan 2 to perform automatic installation of home devices.

The object of the invention is a method for registering a device in a wireless network comprising a central access point characterized in that it comprises the steps of:

-sending an identification code from the device to the access point;

-checking by said access point whether the received identification code corresponds to the identification code sent by said device and if such checking is positive, sending an authentication key from said access point to said device;

-storage of said authentication key by said device for use in authentication procedures between said device and said access point.

According to a preferred embodiment, a unique identification code is used within a given network.

Further characteristics and advantages of the invention will appear through the description of a preferred, non-limiting embodiment of the invention. This embodiment will be described with the help of the following figures, which are an integral part of the present description:

-Figure 1 is a schematic diagram of a network comprising two wired buses communicating through a wireless link.

-Figure 2 is a high-level message sequence chart illustrating the messages exchanged between a Mobile Terminal and an Access Point for creating an association according to the present embodiment.

-Figure 3 is a message sequence chart defining the messages exchanged between different layers of the MT and AP during one of the phases (Information Transfer) defined by the chart of figure 2.

-Figure 4a, 4b and 4c respectively represent a Convergence Layer Information Container for containing Information Elements, and two Information Elements used during the message exchanges of the chart of figure 3.

-Figure 5 is a message sequence chart defining the messages exchanged by the MT and the AP during the authentication phase of the chart of figure 2.

The present embodiment is placed in the frame of BRAN/Hiperlan 2. More information concerning this environment can be found in the following document Broadband Radio Access Networks HIPERLAN Type 2 Functional Specification Data Link Control (DLC) layer parts 1 and 2 (DTS/BRAN030003-1) and associated documents among which the document DTS/BRAN-002004-2 concerning the Radio Link Control (RLC) sublayer.

Figure 1 is a diagram of a network comprising an Access Point (AP) 1 and a Mobile Terminal (MT) 2, respectively connected to wired IEEE 1394 busses 3 and 4. The AP and the MT form a wireless link between the two wired busses.

It is assumed in what follows that the AP (or Central controller CC) is a function that may be implemented in any device. There shall be no prerequisite that there is one fixed AP/CC device in the home network, but rather that one Central Controller is selected among a number of devices having such a capacity.

Before a MT and the AP can associate, a preliminary key negotiation phase must take place in order to generate a symmetric encryption key. This negotiation is based on the Diffie-Hellman (DH) algorithm. The general mechanism of this algorithm is the following :

1. The MT and the AP have agreed on a base generator g and a large prime number n;

2. Both of them generate a random number called the Diffie-Hellman private value. Suppose that the MT generates the number x and the AP generates the number y;
3. The MT computes its DH public value $MT\_DH\_PV=g^x \ mod \ n$ and sends it to the AP;
4. The AP computes its DH public value $AP\_DH\_PV=g^y \ mod \ n$ and sends it to the MT.
5. The MT computes $k=AP\_DH\_PV^x \ mod \ n$;
6. The AP computes $k'=MT\_DH\_PV^y \ mod \ n$.

After this process, the AP and the MT can compute the shared secret session key since $k=k'=g^{xy} \ mod \ n$. For this purpose this key, called Session Secret Key or 'SSK', is computed by :

$SSK=HMAC\text{-}MD5(g^{xy} \ mod \ n,0)$

With :

$HMAC\text{-}MD5(k,m)=MD5((k \ XOR \ opad)|MD5((k \ XOR \ ipad) \ | \ m))$

Where :

- k is a secret key;
- m is the message;
- ipad is 0x36 repeated 64 times;
- opad is 0x5c repeated 64 times;
- XOR is exclusive OR;
- | is the concatenation operator.

Note that if someone eavesdrops on the communication between the MT and the AP, he only learns n, g, MT_DH_PV and AP_DH_PV. Thus, he cannot deduce the value of the key k since he does not know the secret random numbers x and y.

Once the SSK key is generated, the authentication phase can take place. This phase allows the MT to be authenticated by the AP and allows the AP to be authenticated by the MT.

In Hyperlan 2, this step is based on a challenge-response approach :

- The MT sends its identifier to the AP, encrypted with the just negotiated SSK encryption key;
- The AP then sends a challenge (that is a random number) C_{AP} to the MT;
- The MT proves its identity by responding to the challenge C_{AP}. For this purpose, it "signs" the challenge either with a secret key shared with the AP or with its private key when a PKI (*Public Key Infrastructure*) is used. The MT sends its response $R(C_{AP})$ as well as a new challenge C_{MT} to the AP;
- The AP verifies the response $R(C_{AP})$, "signs" the challenge C_{MT} in order to prove its identity and sends back its response $R(C_{MT})$ to the AP;
- The MT verifies the response $R(C_{MT})$.

If the responses $R(C_{AP})$ and $R(C_{MT})$ are correct, both MT and AP are thus authenticated since they proved they know a secret.

In a business environment the authentication is configured by a network administrator. For a home environment, a more automatic authentication procedure is desirable. The interface with the user should be as simple as possible. The 1394 bus per se has "*plug and play*" capabilities, so it is desirable extend these capacities to the wireless network.

An MT wanting to associate with a network needs an authentication key that shall be known by the Central Controller. This authentication key is used during the association phase, via a challenge / response mechanism, in a way similar to that given above. The Hiperlan 2 standardization group thinks

that a single common key may be used for the whole network, and that this key may be based on the GUID of the first Central Controller registered in the network.

Before using a wireless device, an installation phase will be necessary. This phase consists in giving the authentication key of the network to the new MT. According to the present embodiment, this value transfer is secured by a code such as a PIN code to prevent any neighbour from obtaining this key.
It is proposed to use a same PIN code on all the devices for device installation. This PIN code is entered by the user and exchanged over the air interface. It is checked by the CC, that can then communicate the authentication key. The authentication key shall then be stored by the MTs (on non volatile memory), and it will be used at any power on phase to authenticate again.

This method focuses on devices that provide enough user interaction capabilities for entering the PIN code. Typically, such a device comprises a display and a number of keys. The device may provide an installation menu that the user has to select. Upon activation of the installation menu, the device erases any previously stored authentication key. Such devices may also be much simpler. User input may me reduced to the setting of microswitches.

If the device is a CC capable device, then the device shall further ask the user :

---

*A/ do you want to install a new network ?

*B/ do you want to install a device on an existing network ?

If the device is not a CC capable device, then there is no need for this submenu since the user can obviously only connect this device to an existing network.

If the user answers « A », then the device asks for a PIN code. This PIN code will be valid for the whole network. The device then builds an authentication key by concatenating its own GUID (see below) and the entered PIN code. The PIN code is stored in non volatile memory to be retrieved at each power on. The device can then start CC operation (i.e. act as an HL2 Access Point), waiting for further devices.

The GUID is a 64-bit quantity used to uniquely identify an IEEE 1394 device. It consists of a 24-bit company ID (obtained from the 1394 Registration Authority Committee) and a 40-bit serial number assigned by the device manufacturer. The GUID is stored in a device's configuration ROM and is persistent over 1394 network resets.

Other types of identifiers may also be used, as long as it is made sure that no two devices in the network have the same identifier.

If the user answers « B », then the device asks for a PIN code (that shall be the whole network PIN code, the user already initialized on the first installed device). The device then starts MT operation. The MT scans the spectrum, and looks for a beacon under the form of a BRAN frame header. When it finds such a beacon, and after SSK determination, using Link_Info messages, it sends the user entered PIN code to the CC. The user entered PIN code shall be encrypted using the Diffie Hellman session key (the RLC messages are not encrypted). The CC can then check whether the received PIN code (from the air interface) is the same as the one it already has. If the check is successful, then a positive answer is sent through the RLC_INFO_ACK message, with the authentication key (the authentication key is also encrypted using the Diffie-Hellman session key). Otherwise a

denial is sent in the RLC_INFO_ACK. More details of the exchange are given in figure 3.

If the MT receives the authentication key, the installation phase is ready. The MT shall store the key in a non-volatile memory. It could also store the NET_ID (contained in a field of the BCCH) that can help in further frequency scanning. The NET_ID does not uniquely identify a network, but can simplify the frequency scanning and avoid useless authentication tentatives.
It can then further run the power-on, or booting, procedure (see below). If the device does not get the authentication key, it shall look for another frequency, and thus for another CC and try again.

According to the present example, the PIN code and the authentication key are part of the CL_Info container, and thus described for each convergence layer. Another possibility is to make it part of the DLC layer container since it contains data that is relevant to the DLC layer.

Figure 4a represents the convergence layer information container's format (CL_layer_container). It contains several Information Elements (IEs). Figures 4b and 4c represent the formats of two IEs which are needed for the protocol, namely the PIN code IE and the Authentication key IE, and contained in the convergence layer container. The variable 'Authentication_key) is equal to the concatenation of the GUID of the first installed GUID and the PIN code.

The procedure at power on is the following: An MT only device searches for the beacon by scanning the available frequencies. If it previously stored a network identifier (Net_ID), it first searches for the BCCH field containing this identifier. Once the BCCH is found, encryption and authentication steps are

carried out. If the BCCH with the correct Net_ID is is not found, CCs with other identifiers may be searched for.

No specific parameter is needed in the RLC_Authentication message (since a single key is used). The authentication key (GUID + PIN code) is used by the MT to compute the challenge response sent in the RLC_Authentication_AP message. The same authentication key (GUID + PIN code) is used by the AP/CC to check whether the device is allowed or not (whether it shares the same key), and thus to generate the response.
If the MT is authenticated, then it can complete the association phase and join the network. Otherwise it tries on another CC.
Figure 5 describes the message exchange of the authentication procedure.

The described method may be extended to multiple authentication keys.
The major drawback of the present approach appears to uninstall some devices : when the user wants to remove only part of his devices (at least one stolen device), he has to change the pin code, and to reinstall all his wireless devices.
This drawback disappears when one authentication key is used for each device.
The same procedures and message sets can be used for a multiple authentication key network with the following modifications:

-Installation phase :
During installation, the MT has to send its GUID to the CC. The MT GUID concatenated to the PIN code is the MT authentication key. The authentication_key IE can be used (or even a new information element can be defined, without the Accept/denied flag), and can be carried in the RLC_INFO message. The Authentication key sent in the RLC_INFO message has to be encrypted using the Diffie-Hellman session key.

The PIN code is used by the CC to check whether the MT is allowed to be installed. If the PIN code test matches, then the authentication key of the MT is stored by the CC in non volatile memory.

The RLC_INFO_ACK in that case just contains the accept/denied flag. No authentication key is needed.

-Power on phase

During Authentication phase, the RLC_Authentication message sent by the MT to the CC shall contain the authentication ID of the MT (which is the GUID of the MT). Then the authentication key to be used for the challenge / response exchange shall be the MT GUID concatenated to the PIN code.

This approach allows a user to remove one device without needing to reinstall his complete network.

The invention has several advantages. User involvement is reduced to just entering a PIN code during device installation. Also, the PIN code provides a good level of security for device installation and guarantees that devices are wirelessly installed to the appropriate network

GLOSSARY

ACF	Association Control Function
BCCH	Broadcast Control CHannel
CL	Convergence Layer
DLC	Data Link Control Layer
ENV	Environment Layer (Convergence Layer)
GUID	Global Unique Identifier
MAC	Medium Access Control
NET_ID	Network Identifier
PHY	Physical Layer
PIN	Personal Identification Number
RLC	Radio Link Control Protocol
SSK	Session Secret Key

CLAIMS

1. Method for registering a device in a wireless network comprising a central access point characterized in that it comprises the steps of:
-sending an identification code from the device to the access point;
-checking by said access point whether the received identification code corresponds to the identification code sent by said device and if such checking is positive, sending an authentication key from said access point to said device;
-storage of said authentication key by said device for use in authentication procedures between said device and said access point.

2. Method according to claim 1, characterized in that a unique identification code is used within a given network.

Abstract

The invention concerns a method for registering a device in a wireless network comprising a central access point.

The method comprises the steps of

-sending an identification code from the device to the access point;

-checking by said access point whether the received identification code corresponds to the identification code sent by said device and if such checking is positive, sending an authentication key from said access point to said device;

-storage of said authentication key by said device for use in authentication procedures between said device and said access point.

The invention is applicable among others in digital home networks.

Figure 2

THIS PAGE BLANK (USPTO)

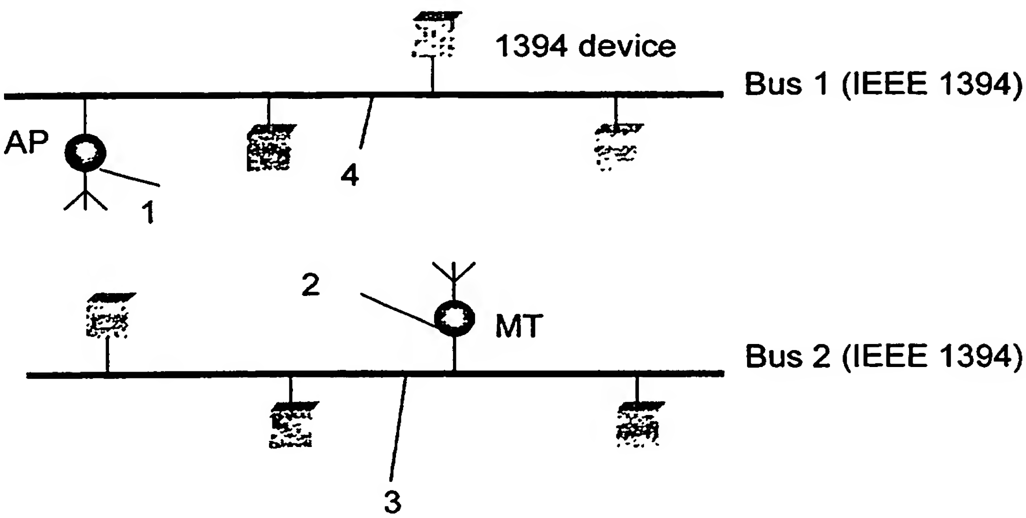

Fig. 1

MSC Association_new

1(1)

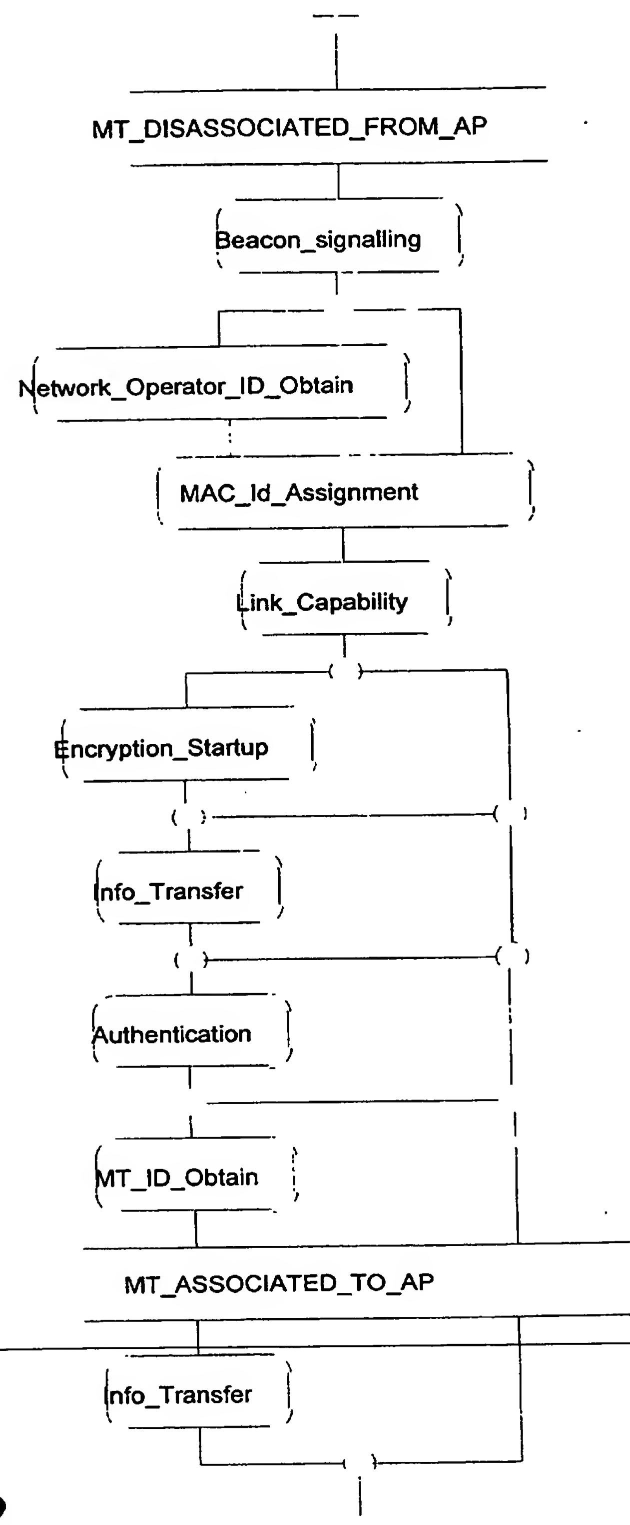

Fig. 2

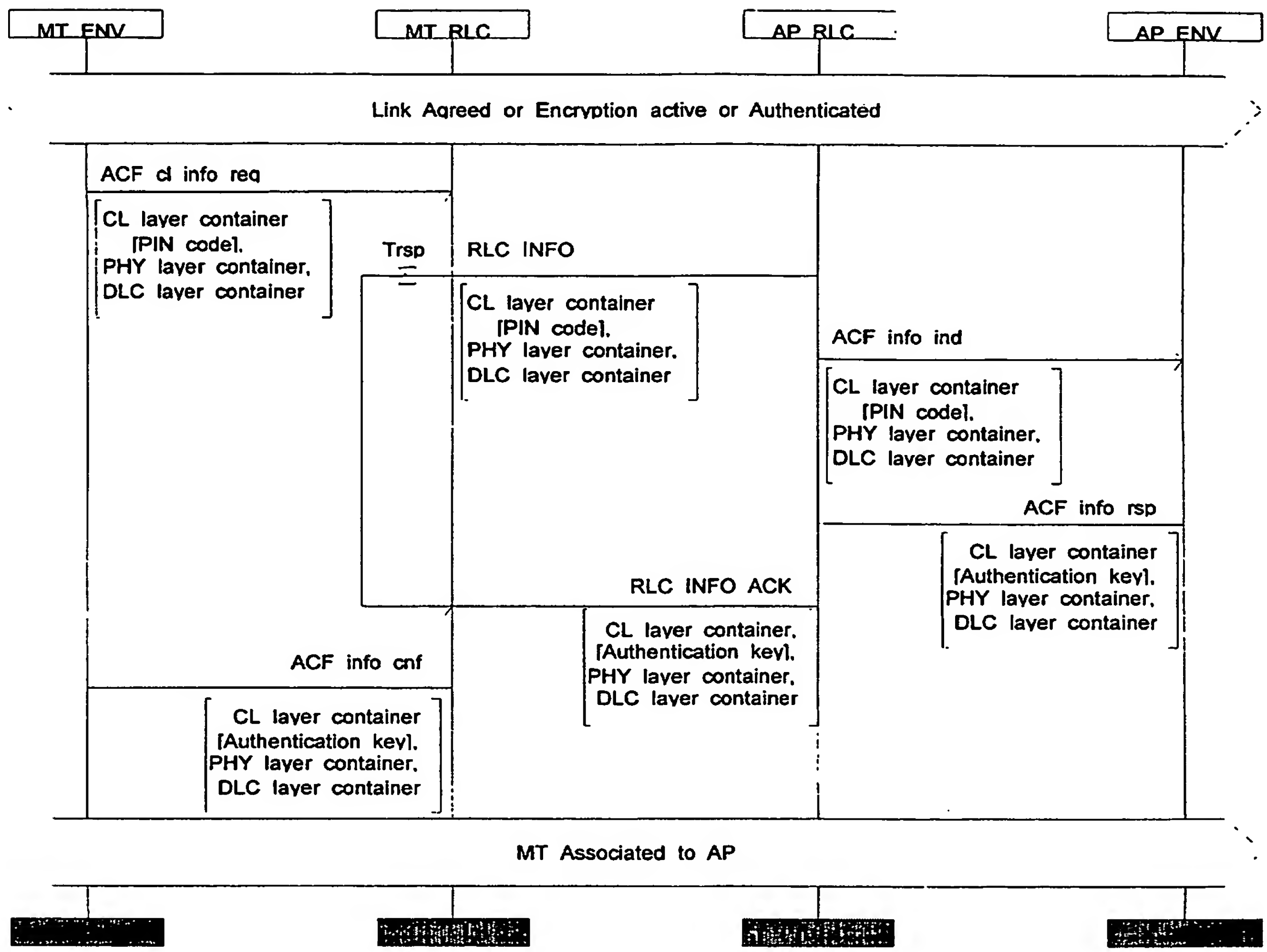
MT ENV
MT RLC
AP RLC
AP ENV
Link Agreed or Encryption active or Authenticated
ACF cl info req
CL layer container [PIN code], PHY layer container, DLC layer container
Trsp
RLC INFO
CL layer container [PIN code], PHY layer container, DLC layer container
ACF info ind
CL layer container [PIN code], PHY layer container, DLC layer container
ACF info rsp
CL layer container [Authentication key], PHY layer container, DLC layer container
RLC INFO ACK
CL layer container, [Authentication key], PHY layer container, DLC layer container
ACF info cnf
CL layer container [Authentication key], PHY layer container, DLC layer container
MT Associated to AP

Fig. 3

Bits

8 7 6 5 4 3 2 1		Octets
IE Type		1
Reserved	Length (L)	2
Information		3 .. L + 2

Fig. 4a

Bits

8 7 6 5 4 3 2 1		Octets
Pin_Code IE Type		1
Reserved	Length (L)	2
SSK(Pin1| Pin2 | Pin3 | Pin4)		

Fig. 4b

Bits

8 7 6 5 4 3 2 1		Octets
Authentication_key IE Type		1
Reserved	Length (L)	2
Accept or denied flag		
If Accept : SSK(Authentication_key)		

Fig. 4c

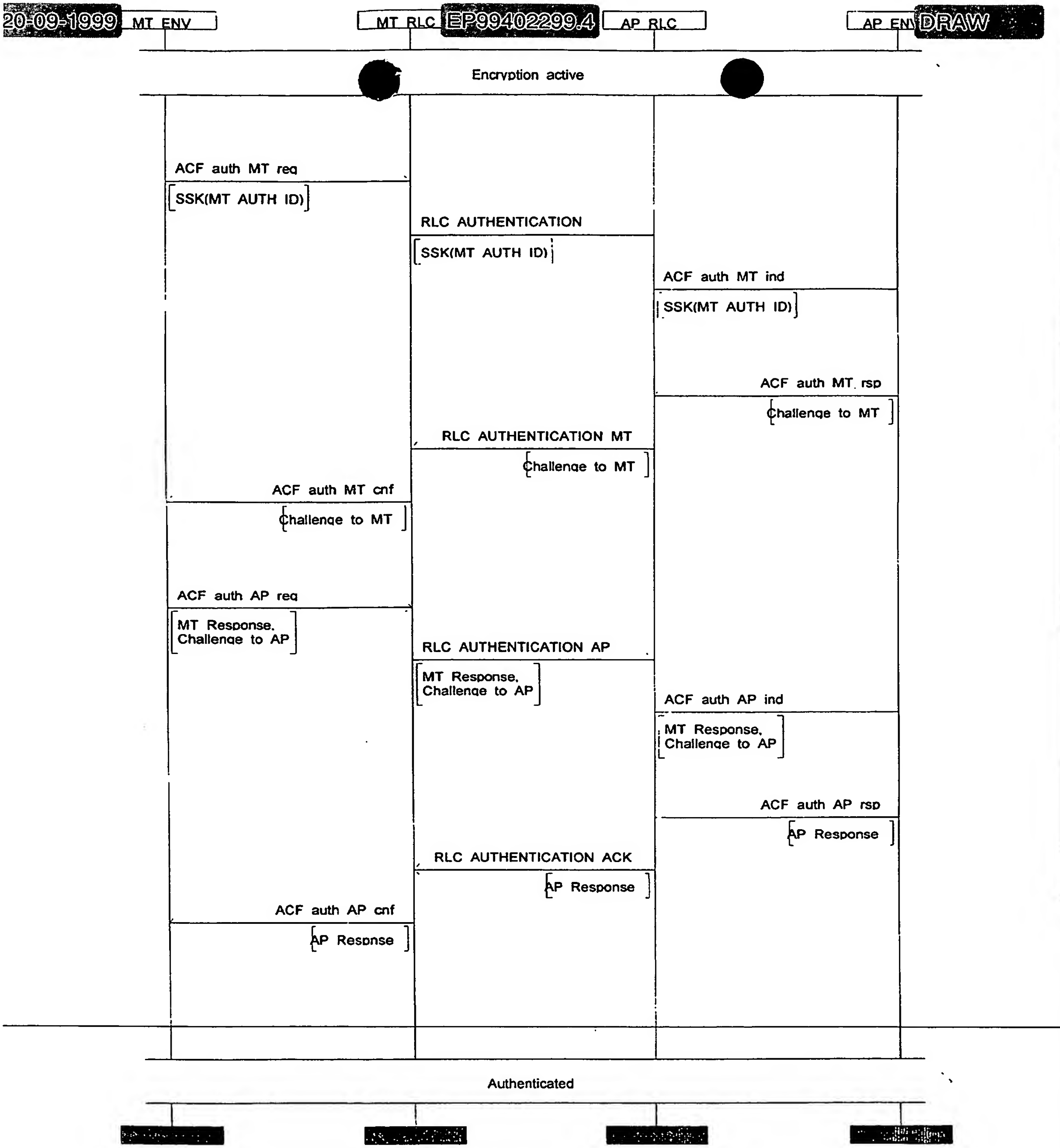
MT ENV
MT RLC
AP RLC
AP ENV
Encryption active
ACF auth MT req
SSK(MT AUTH ID)
RLC AUTHENTICATION
SSK(MT AUTH ID)
ACF auth MT ind
SSK(MT AUTH ID)
ACF auth MT rsp
Challenge to MT
RLC AUTHENTICATION MT
Challenge to MT
ACF auth MT cnf
Challenge to MT
ACF auth AP req
MT Response,
Challenge to AP
RLC AUTHENTICATION AP
MT Response,
Challenge to AP
ACF auth AP ind
MT Response,
Challenge to AP
ACF auth AP rsp
AP Response
RLC AUTHENTICATION ACK
AP Response
ACF auth AP cnf
AP Response
Authenticated

Fig. 5